(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年11 月25 日 (25.11.2004)

PCT

(10) 国際公開番号
WO 2004/102886 A1

(51) 国際特許分類[7]: H04L 12/28

(21) 国際出願番号: PCT/JP2004/004919

(22) 国際出願日: 2004 年4 月5 日 (05.04.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-138552 2003 年5 月16 日 (16.05.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 五十嵐 卓也 (IGARASHI, Tatsuya) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 吉川 典史 (KIKKAWA, Norifumi) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 小堀 洋一 (KOBORI, Yoichi) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 森田 岳彦 (MORITA, Takehiko) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 本田 康晃 (HONDA, Yasuaki) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 田中 浩一 (TANAKA, Koichi) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

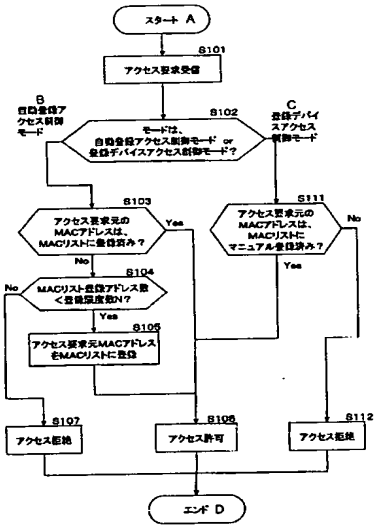
(74) 代理人: 宮田 正昭, 外(MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目1番7号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE, ACCESS CONTROL PROCESSING METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラム



A...START
S101...RECEIVE ACCESS REQUEST
B...AUTOMATIC REGISTRATION ACCESS CONTROL MODE
S102...IS MODE AUTOMATIC REGISTRATION ACCESS CONTROL MODE OR REGISTRATION DEVICE ACCESS CONTROL MODE?
C...REGISTRATION DEVICE ACCESS CONTROL MODE
S103...IS MAC ADDRESS OF ACCESS REQUESTOR ENTERED IN MAC LIST?
S111...IS MAC ADDRESS OF ACCESS REQUESTOR MANUALLY REGISTERED ON MAC LIST?
S104...NUMBER OF ADDRESSES ENTERED IN MAC LIST REGISTRATION LIMIT NUMBER N?
S105...ENTER MAC ADDRESS OF ACCESS REQUESTOR WITH MAC LIST
S107...REJECT ACCESS
S106...ALLOW ACCESS
S112...REJECT ACCESS
D...END

(57) Abstract: A device and a method for controlling access differently according to a mode setting. A MAC address table in which a manual registration MAC address and an automatic registration MAC address are entered in an identifiable form is set. When the access control mode is an automatic registration access control mode, access request client MAC addresses are registered until the number of access request client MAC adresses reaches the predetermined registration limit number N of the MAC address table, and access is allowed under the condition that the access client MAC address is registered. When the access control mode is a registration device access control mode, access is allowed under the condition that the client MAC address is entered in the MAC address table as a manual registration MAC address.

(57) 要約: モード設定による異なるアクセス制御を可能とした装置および方法を実現する。マニュアル登録ＭＡＣアドレスと、自動登録ＭＡＣアドレスとを識別可能な態様で登録したＭＡＣアドレステーブルを設定し、アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントＭＡＣアドレスを、ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、登録を条件としてアクセスを許容し、アクセス制御モードが、登録デバイスアクセス制御モードである場合は、クライアントＭＡＣアドレスが、ＭＡＣアドレステーブルに、マニュアル登録ＭＡＣアドレスとして設定されていることを条件としてアクセスを許容する。

WO 2004/102886 A1

BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明　細　書

情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラム

技術分野

本発明は、情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、ネットワーク接続された機器間の通信においてアクセス権限判定に基づくアクセス制御処理を実行する情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラムに関する。

背景技術

昨今のデータ通信ネットワークの普及に伴い、家庭内においても家電機器やコンピュータ、その他の周辺機器をネットワーク接続し、各機器間での通信を可能とした、いわゆるホームネットワークが浸透しつつある。ホームネットワークは、ネットワーク接続機器間で通信を行なうことにより各機器のデータ処理機能を共有したり、機器間でコンテンツの送受信を行なう等、ユーザに利便性・快適性を提供するものであり、今後、ますます普及することが予測される。

このようなホームネットワークの構成に適するプロトコルとしてＵＰｎＰ（登録商標）が知られている。ＵＰｎＰは、複雑な操作を伴うことなく容易にネットワークを構築することが可能であり、困難な操作や設定を伴うことなくネットワーク接続された機器において各接続機器の提供サービスを受領可能とするものである。また、ＵＰｎＰはデバイス上のＯＳ（オペレーティングシステム）にも依存せず、容易に機器の追加ができるという利点を持つ。

ＵＰｎＰは、接続機器間で、ＸＭＬ（eXtensible Markup Language）に準拠した定義ファイルを交換し、機器間において相互認識を行なう。ＵＰｎＰの処理の概要は、以下の通りである。

（１）ＩＰアドレス等の自己のデバイスＩＤを取得するアドレッシング処理。

（２）ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理。

（３）ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理。

上記処理手順を行なうことで、ネットワーク接続された機器を適用したサービスの提供および受領が可能となる。ネットワークに新たに接続される機器は、上記のアドレッシング処理によりデバイスＩＤを取得し、ディスカバリ処理によりネットワーク接続された他のデバイスの情報を取得して、取得情報に基づいて他の機器にサービスの要求が可能となる。

しかし、一方、この種のネットワークでは、不正アクセスに対する対策を考慮することも必要となる。ホームネットワーク内の機器、例えばサーバ等には私的なコンテンツや有料コンテンツ等の著作権管理を要求されるコンテンツが格納されることも多い。

このようなホームネットワーク内のサーバに格納されたコンテンツは、ネットワーク接続された他の機器からアクセス可能となる。例えば、上述の簡易な機器接続構成であるＵＰｎＰ接続を実行した機器によってコンテンツを取得することが可能となる。コンテンツが映画データや音楽データの場合、ネットワーク接続機器としてＴＶ、あるいはプレーヤ等を接続すれば、映画を視聴したり、音楽を聴いたりすることが可能となる。

コンテンツの利用権を有するユーザの接続した機器によるアクセスは許容

されてもよいが、上述のようなネットワーク構成においては、コンテンツ等の利用権を持たないユーザがネットワークに入り込むことも容易である。例えば無線ＬＡＮによって構成されたネットワークの場合には家の中にあるサーバに対して、戸外、あるいは隣家等から通信機器を利用して不正にネットワークに参入し、コンテンツの搾取を行なうような事態も発生し得る。このような不正なアクセスを許容する構成は、秘密漏洩を生じさせることにもなり、また、コンテンツ著作権の管理の観点からも重要な問題となる。

上述のような不正アクセスを排除するため、例えばサーバにアクセスを許容するクライアントのリストを保持させ、クライアントからサーバに対するアクセス要求の際に、サーバでリストとの照合処理を実行して不正アクセスを排除する構成が提案されている。

例えば、ネットワーク接続機器に固有の物理アドレスであるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスを、アクセス許容機器リストとして設定するＭＡＣアドレスフィルタリングが知られている。ＭＡＣアドレスフィルタリングとは、ホームネットワーク等の内部ネットワーク（サブネット）と外部ネットワークとを隔離するルータあるいはゲートウェイに、予めアクセスを許容するＭＡＣアドレスを登録しておき、受信したパケットのＭＡＣアドレスと登録されたＭＡＣアドレスとを照合し、登録されていないＭＡＣアドレスを有する機器からのアクセスを拒否するものである。なお、この種の技術については、例えば特開平１０－２７１１５４号公報（特許文献１）に開示されている。

しかし、一般にアクセス制限をするためのＭＡＣアドレスの登録処理を行なうためには、ユーザあるいは管理者がネットワークに接続される機器のＭＡＣアドレスを調べて、調べたＭＡＣアドレスをオペレータが入力してリストを作成するという処理が必要となる。

ホームネットワークにおいては、新たな機器の追加処理が行われることは頻繁に発生することであり、このような機器追加処理の際に、ユーザが逐次、機器のＭＡＣアドレスを調べて登録処理をしなければならないとすると、ネットワーク構築の容易性を阻害することになる。

一方、一般家庭においても、ＰＣのみならず、家電機器も含んだネットワーク構成が構築され、どのような機器からでもネットワークにアクセス可能ないわゆるユビキタス環境が構築されつつあり、また、無線ＬＡＮ等の普及により、通信可能な機器が外部から無線ＬＡＮに侵入することも容易となっている。このようなネットワーク環境において、ネットワーク接続機器に対する不正アクセスもより発生しやすくなっており、不正なアクセスによる秘密情報の搾取、コンテンツの不正読み取り等が実行される可能性はますます高くなっている。このような状況において、一般ユーザに負担を強いることなく、適切なアクセス制御構成を容易に実現することが求められている。

発明の開示

本発明は、上述の問題点に鑑みてなされたものであり、様々な機器からのアクセス要求をネットワークを介して受領する情報処理装置におけるアクセス制御において、複数のモードに基づく異なる態様でのアクセス制御処理を可能とすることで、ユーザ負担の軽減を図るとともに、不特定多数クライアントからの無制限なアクセスについても防止可能とした情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

本発明の第１の側面は、

アクセス制御処理を実行する情報処理装置であり、

マニュアル登録のなされたクライアントＭＡＣアドレスと、自動登録処理のなされたクライアントＭＡＣアドレスとを識別可能な態様で登録したＭＡＣ

アドレステーブルを記憶した記憶部と、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかに応じて、クライアントからのアクセス要求に対して異なるアクセス制御処理を実行するアクセス制御部とを有し、

前記アクセス制御部は、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスを、前記ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

情報処理装置に設定されたアクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスが、前記ＭＡＣアドレステーブルに、マニュアル登録されたＭＡＣアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行する構成を有することを特徴とする情報処理装置にある。

さらに、本発明の情報処理装置の一実施態様において、前記アクセス制御部は、情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合、クライアントのアクセス要求種別を識別し、該識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別である場合にのみ、クライアントのＭＡＣアドレスを、前記ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容する処理を実行する構成であることを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記アクセス制御を実行すべき要求種別は、ＨＴＴＰ(Hyper Text Transfer Protocol)－ＧＥＴメソッドに基づくコンテンツ要求処理、またはＳＯＡＰ（Simple Object Access Protocol)に基づく制御要求処理の少なくともいずれかを含むことを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、クライアントＭＡＣアドレスを前記ＭＡＣアドレステーブルにマニュアル登録のなされたクライアントＭＡＣアドレスとして登録する処理を実行する登録処理部を有することを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記ＭＡＣアドレステーブルに自動登録のなされたクライアントＭＡＣアドレスとして登録されたＭＡＣアドレスについて、予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、前記ＭＡＣアドレステーブルの自動登録クライアントＭＡＣアドレスエントリをマニュアル登録クライアントＭＡＣアドレスエントリとする設定変更処理を実行する登録処理部を有することを特徴とする。

さらに、本発明の第２の側面は、

情報処理装置におけるアクセス制御処理方法であり、

クライアントからのアクセス要求を受信するアクセス要求受信ステップと、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかを判定するモード判定ステップと、

設定アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスを、ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

設定アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスが、前記ＭＡＣアドレステーブルに、マニュアル登録されたＭＡＣアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行するアクセ

ス制御ステップと、

を有することを特徴とするアクセス制御処理方法にある。

さらに、本発明のアクセス制御処理方法の一実施態様において、前記アクセス制御ステップは、情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合、クライアントのアクセス要求種別を識別し、該識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別である場合にのみ、クライアントのＭＡＣアドレスを、前記ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容する処理を実行することを特徴とする。

さらに、本発明のアクセス制御処理方法の一実施態様において、前記アクセス制御を実行すべき要求種別は、ＨＴＴＰ(Hyper Text Transfer Protocol)－ＧＥＴメソッドなどに基づくコンテンツ要求処理、またはＳＯＡＰ（Simple Object Access Protocol）に基づく制御要求処理の少なくともいずれかを含むことを特徴とする。

さらに、本発明のアクセス制御処理方法の一実施態様において、前記アクセス制御処理方法は、さらに、予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、クライアントＭＡＣアドレスを前記ＭＡＣアドレステーブルにマニュアル登録のなされたクライアントＭＡＣアドレスとして登録する処理を実行する登録処理ステップを有することを特徴とする。

さらに、本発明のアクセス制御処理方法の一実施態様において、前記アクセス制御処理方法は、さらに、前記ＭＡＣアドレステーブルに自動登録のなされたクライアントＭＡＣアドレスとして登録されたＭＡＣアドレスについて、予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、前記ＭＡＣアドレステーブルの自動登録ク

ライアントＭＡＣアドレスエントリをマニュアル登録クライアントＭＡＣアドレスエントリとする設定変更処理を実行する登録処理ステップを有することを特徴とする。

さらに、本発明の第３の側面は、

情報処理装置におけるアクセス制御処理を実行するコンピュータ・プログラムであり、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかを判定するモード判定ステップと、

設定アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスを、ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

設定アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスが、前記ＭＡＣアドレステーブルに、マニュアル登録されたＭＡＣアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行するアクセス制御ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

本発明の構成においては、マニュアル登録のなされたクライアントＭＡＣアドレスと、自動登録処理のなされたクライアントＭＡＣアドレスとを識別可能な態様で登録したＭＡＣアドレステーブルを設定し、アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスを、ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスが、ＭＡＣアドレステ

ーブルに、マニュアル登録されたＭＡＣアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行する構成としたので、ユーザによるマニュアル登録処理を実行しない場合においても、無制限なアクセスが防止され、例えば不特定多数クライアントからのサーバ格納コンテンツの取得等を防止することが可能となり、さらに、モードを、登録デバイスアクセス制御モードに設定することにより、厳格なアクセス制御を実行することも可能となる。

さらに、本発明の構成によれば、自動登録アクセス制御モードにおいて、クライアントのアクセス要求種別を識別し、識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別、例えばＨＴＴＰ(Hyper Text Transfer Protocol)－ＧＥＴメソッドに基づくコンテンツ要求処理、またはＳＯＡＰ（Simple Object Access Protocol）に基づく制御要求処理である場合にのみ、クライアントのＭＡＣアドレスを、ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としたアクセス許容を実行する構成としたので、ＵＰｎＰ等における機器発見処理、情報取得処理等において不必要なアクセス制御を行うことが防止される。

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づく、より詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装

置が同一筐体内にあるものには限らない。

図面の簡単な説明

図１は、本発明の適用可能なネットワーク構成例を示す図である。

図２は、ネットワーク接続機器の構成例について説明する図である。

図３は、本発明の情報処理装置の有するＭＡＣアドレステーブルおよびアクセス制御処理について説明する図である。

図４は、本発明の情報処理装置の実行するアクセス制御処理について説明するフロー図である。

図５は、クライアントが送信するパケット構成を示す図である。

図６は、本発明の情報処理装置の実行するアクセス制御処理について説明するフロー図である。

図７は、本発明の情報処理装置のアクセス制御処理構成を示す機能ブロック図である。

図８は、アクセス制御処理を実行する情報処理装置のディスプレイに表示されるユーザインタフェース構成例を示す図である。

図９は、クライアントからのアクセス要求に含まれるＨＴＴＰ－ＧＥＴヘッダのデータ例を示す図である。

図１０は、ＭＡＣアドレスのマニュアル登録処理シーケンスの例を示すシーケンス図である。

図１１は、サーバの機能構成を示すブロック図である。

図１２は、クライアントの機能構成を示すブロック図である。

発明を実施するための最良の形態

以下、図面を参照しながら、本発明の情報処理装置、およびアクセス制御処理方法、並びにコンピュータ・プログラムの詳細について説明する。

[システム概要およびＭＡＣアドレステーブル]

まず、図１を参照して、本発明の適用可能なネットワーク構成例について説明する。図１は、様々なクライアント機器からの処理要求に応じて処理を実行するサーバ１０１と、サーバ１０１に対して処理要求を行なうクライアント機器としてのＰＣ１２１，１２２，１２４、ＰＤＡ、携帯電話等の携帯通信端末１２３，１２５がネットワーク１００を介して接続された構成、例えばホームネットワーク構成を示している。

サーバ１０１がクライアントからの要求に応じて実行する処理は、例えばサーバ１０１の保有するハードディスク等の記憶手段に格納されたコンテンツの提供、あるいはサーバの実行可能なアプリケーションプログラムの実行によるデータ処理サービス等である。なお、図１においては、サーバ１０１と、その他のクライアント機器としてのＰＣ１２１，１２２，１２４、ＰＤＡ、携帯電話等の携帯通信端末１２３，１２５とを区別して示しているが、クライアントからの要求に対するサービスを提供する機器をサーバとして示しているものであり、いずれのクライアント機器も、自己のデータ処理サービスを他のクライアントに提供する場合には、サーバとしての機能を提供可能となる。従って、図１に示すネットワーク接続されたクライアント機器もサーバとなり得る。

ネットワーク１００は、有線、無線等いずれかのネットワークであり、各接続機器は、ＭＡＣ(Media Access Control)アドレスを有している。各ネットワーク接続機器は、宛先ＭＡＣアドレスおよび送信元ＭＡＣアドレスをヘッダ情報に持つパケット、例えばイーサネット（登録商標）フレームをネットワーク１００を介して送受信する。すなわち、クライアントは、イーサネットフレームのデータ部に処理要求情報を格納したフレームをサーバ１０１に送信することにより、サーバ１０１に対するデータ処理要求を実行する。サーバ１０１は、処理要求フレームの受信に応じて、後述するアクセス権限判定処理を行ない、権限ありの判定を条件としてデータ処理を実行し、必要に応じてデータ処理結果としての結果データをイーサネットフレームのデータ部に格納し、各ク

ライアントに送信する。

ネットワーク接続機器は、例えばユニバーサルプラグアンドプレイ（ＵＰｎＰ：Universal Plug and Play）対応機器によって構成される。従って、ネットワークに対する接続機器の追加、削除が容易な構成である。ネットワークに新たに接続する機器は、

（１）ＩＰアドレス等の自己のデバイスＩＤを取得するアドレッシング処理。

（２）ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理。

（３）ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理。

上記処理手順を行なうことで、ネットワーク接続された機器を適用したサービスを受領することが可能となる。

図１に示すサーバおよびクライアント機器を構成するＰＣ等の情報処理装置のハードウェア構成例について図２を参照して説明する。

ＣＰＵ(Central Processing Unit)３０１は、ＲＯＭ(Read Only Memory)３０２、またはＨＤＤ３０４等に記憶されているプログラムに従って、各種の処理を実行し、データ処理手段、あるいは通信制御処理手段として機能する。ＲＡＭ３０３には、ＣＰＵ３０１が実行するプログラムやデータが適宜記憶される。ＣＰＵ３０１、ＲＯＭ３０２、およびＲＡＭ３０３、ＨＤＤ３０４は、バス３０５を介して相互に接続されている。

バス３０５には、入出力インタフェース３０６が接続されており、この入出力インタフェース３０６には、例えば、ユーザにより操作されるキーボード、スイッチ、ボタン、あるいはマウス等により構成される入力部３０７、ユーザに各種の情報を提示するＬＣＤ、ＣＲＴ、スピーカ等により構成される出力部

３０８が接続される。さらに、データ送受信手段として機能する通信部３０９、さらに、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどのリムーバブル記録媒体３１１を装着可能で、これらのリムーバブル記録媒体３１１からのデータ読み出しあるいは書き込み処理を実行するドライブ３１０が接続される。

図２に示す構成は、図１に示すネットワーク接続機器の一例としてのサーバ、パーソナルコンピュータ（ＰＣ）の例であるが、ネットワーク接続機器はＰＣに限らず、図１に示すように携帯電話、ＰＤＡ等の携帯通信端末、その他の様々な電子機器、情報処理装置によって構成することが可能である。従って、それぞれの機器固有のハードウェア構成を持つことが可能であり、そのハードウェアに従った処理を実行する。

本発明において、アクセス制御を行なうネットワーク接続機器としての情報処理装置は、アクセス権限を有するネットワーク接続機器の機器リストとしてアクセス権限を有するネットワーク接続機器のＭＡＣアドレスを登録したＭＡＣアドレステーブルを格納し、ＭＡＣアドレステーブルに基づくアクセス制御処理を実行する。

ＭＡＣアドレステーブルに基づくアクセス制御を実行する情報処理装置は、２つのアクセス制御モードを持つ。すなわち、

（１）自動登録アクセス制御モード

（２）登録デバイスアクセス制御モード

の２つのモードである。

（１）自動登録アクセス制御モードは、ＭＡＣアドレステーブルに基づくアクセス制御を実行する情報処理装置が、外部機器（クライアント）からのアクセス要求を受信した場合に、アクセス要求パケットから送信元ＭＡＣアドレス（クライアントＭＡＣアドレス）を取得し、情報処理装置に格納したＭＡＣア

ドレステーブルに登録された登録済みＭＡＣアドレスと一致するか否かを判定し、一致する場合には、アクセスを許可する。一致しない場合には、アクセス要求パケットから取得したＭＡＣアドレスをＭＡＣアドレステーブルに自動登録し、登録処理が実行されたことを条件としてアクセスを許容する。

ただし、ＭＡＣアドレステーブルに対するＭＡＣアドレス登録数には予め登録限度数：Ｎ（例えばＮ＝５，１０，１５，６３など）が設定され、ＭＡＣアドレステーブルの登録ＭＡＣアドレス数が登録限度数：Ｎに達していない場合に限り、ＭＡＣアドレスの自動登録処理が実行され、自動登録処理の後、アクセスが許可される。

（２）登録デバイスアクセス制御モードは、ＭＡＣアドレステーブルに基づくアクセス制御を実行する情報処理装置が、外部機器（クライアント）からのアクセス要求を受信した場合に、アクセス要求パケットから送信元ＭＡＣアドレス（クライアントＭＡＣアドレス）を取得し、情報処理装置に格納したＭＡＣアドレステーブルに登録された登録済みＭＡＣアドレス中、予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理がなされたマニュアル登録ＭＡＣアドレスと一致するか否かを判定し、マニュアル登録ＭＡＣアドレスと一致する場合には、アクセスを許可する。一致しない場合には、アクセスを許可しない処理を実行するモードである。

本発明の情報処理装置においては、上記２つのモードを適宜切り替えることを可能とし、各設定モードにおいて、上記態様でのアクセス制御を行う。

本発明の情報処理装置がアクセス制御を行うために、記憶部に格納するＭＡＣアドレステーブル（ＭＡＣリスト）の構成例について、図３を参照して説明する。アクセス制御を行なうネットワーク接続機器としての情報処理装置４１０は、ネットワークを介して接続される様々な情報処理装置４２１～４２３からアクセス要求を受領し、そのアクセス要求に含まれる送信元ＭＡＣアドレス

と、ＭＡＣアドレステーブル（ＭＡＣリスト）４１１に格納されたＭＡＣアドレスとの照合を行う。

情報処理装置４１０が記憶部に格納しているＭＡＣアドレステーブル（ＭＡＣリスト）４１１は、図に示すように、登録限度数：Ｎまでのエントリを格納することを許容したテーブル構成を持ち、上述の自動登録アクセス制御モードまたは、予め定められたシーケンスに従ってマニュアル登録がなされたＭＡＣアドレスデータが格納されている。

さらに、ＭＡＣアドレステーブル（ＭＡＣリスト）４１１には、登録ＭＡＣアドレスがマニュアル登録されたデータであるか否かのデータが各ＭＡＣアドレスに対応付けられたデータとして設定される。

すなわち、予め設定された登録シーケンスに従ったマニュアル登録処理によって登録されたＭＡＣアドレスであるか、あるいは上述の自動登録アクセス制御モードにおいて自動登録されたアドレスであるかを示すマニュアル登録識別データが、ＭＡＣアドレステーブル４１１に各登録ＭＡＣアドレスに対応して設定される。図３において、マニュアル登録欄に○の設定されたエントリが予め設定された登録シーケンスに従ったマニュアル登録処理によって登録されたＭＡＣアドレスである。

ＭＡＣアドレステーブルは、アクセス制御を行なうネットワーク接続機器としての情報処理装置（サーバ）内の記憶部（不揮発性メモリ）に格納される。ＭＡＣアドレステーブルは、スロット単位で、各クライアントの登録データを格納する構成を有し、１スロット毎に１つの登録クライアント情報を格納する。なお、登録情報には、図に示すようにクライアントのＭＡＣアドレスと、マニュアル登録か否かの情報の他、図には示していないが、ユーザが任意に設定可能なクライアント名、登録日時等の情報を格納してもよい。

[モードに応じたアクセス制御処理]

次に、アクセス制御を行なうネットワーク接続機器としての情報処理装置が実行するアクセス制御処理シーケンスについて図４のフローを参照して説明する。

ステップＳ１０１において、アクセス制御を行なうネットワーク接続機器としての情報処理装置は、他のネットワーク接続機器からのアクセス要求を受信する。アクセス制御を行なうネットワーク接続機器としての情報処理装置をサーバ、アクセス要求を実行する情報処理装置をクライアントとして説明する。

クライアントから送信されるアクセス要求パケット（イーサネットフレーム）の構成例を図５に示す。パケットは、ヘッダ部、データ部、トレーラ部に区分され、ヘッダ部には、同期信号、パケット開始符号、宛先ＭＡＣアドレス、送信元ＭＡＣアドレス、およびパケット長，タイプが含まれる。

データ部には、例えばＴＣＰ／ＩＰ通信プロトコルに従って生成されたデータが含まれ、例えば送信元、送信先ＩＰアドレスを含むＩＰパケットが格納される。

サーバは自己のアクセス制御モードが（１）自動登録アクセス制御モード、（２）登録デバイスアクセス制御モードのいずれにあるかによって異なる処理を実行することになる。サーバはステップＳ１０２において自己のモードを識別し、（１）自動登録アクセス制御モードにある場合は、ステップＳ１０３以下の処理を実行する。

ステップＳ１０３では、クライアントからの受信パケットからアクセス要求元のＭＡＣアドレスを取得し、サーバの記憶部に格納したＭＡＣアドレステーブル（図３参照）に登録されたＭＡＣアドレスとの照合処理を実行し、登録済みか否かを判定する。登録済みである場合（ステップＳ１０３：Ｙｅｓ）は、

ステップＳ１０６に進み、アクセスを許可し、クライアントの要求に応じた処理を実行する。

登録済みでない場合（ステップＳ１０３：Ｎｏ）は、ステップＳ１０４に進み、ＭＡＣアドレステーブルにすでに登録されたＭＡＣアドレスがサーバに設定した登録限度数：Ｎに達していないか、すなわち、登録ＭＡＣアドレス＜登録限度数：Ｎであるか否かを判定する。

登録ＭＡＣアドレス＜登録限度数：Ｎである場合（ステップＳ１０４：Ｙｅｓ）は、クライアントからの受信パケットのヘッダ部に設定されている送信元ＭＡＣアドレスをＭＡＣアドレステーブルに登録し、その後、ステップＳ１０６においてアクセスを許可し、クライアントの要求に応じた処理を実行する。

登録ＭＡＣアドレス＜登録限度数：Ｎでない場合（ステップＳ１０４：Ｎｏ）、すなわち、ＭＡＣアドレステーブルに既に登録限度数：ＮのＭＡＣアドレスが登録済みである場合は、これ以上の自動登録を実行できないので、ＭＡＣアドレスの登録処理を実行することなく、ステップＳ１０７において、クライアントからのアクセス要求を拒絶する。

一方、ステップＳ１０２において、自己のモードが、（２）登録デバイスアクセス制御モードであると判定した場合は、ステップＳ１１１に進み、クライアントからの受信パケットからアクセス要求元のＭＡＣアドレスを取得し、サーバの記憶部に格納したＭＡＣアドレステーブル（図３参照）に登録されたＭＡＣアドレス中、予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理がなされたマニュアル登録ＭＡＣアドレスと一致するか否かを判定する。

すなわち、図３において、マニュアル登録欄に○の設定されたエントリのみが照合処理対象のＭＡＣアドレスエントリとなる。送信元ＭＡＣアドレス（ク

ライアントＭＡＣアドレス）が、マニュアル登録されたＭＡＣアドレスエントリと一致する場合（ステップＳ１１１：Ｙｅｓ）には、ステップＳ１０６に進み、アクセスを許可し、クライアントの要求に応じた処理を実行する。

一方、送信元ＭＡＣアドレスが、マニュアル登録されたＭＡＣアドレスエントリと一致しない場合（ステップＳ１１１：Ｎｏ）には、ステップＳ１１２に進み、アクセスを拒絶する。

登録デバイスアクセス制御モードにある場合は、送信元ＭＡＣアドレスが、ＭＡＣアドレステーブルに自動登録されたＭＡＣアドレスと一致する場合であってもアクセスを拒絶することになる。

なお、アクセス制御を行なうネットワーク接続機器としての情報処理装置（サーバ）が（１）自動登録アクセス制御モードにある場合、サーバは、クライアントからの要求態様を判定し、特定のカテゴリのアクセス要求である場合にのみ、アクセス制御を実行、すなわち、ＭＡＣアドレステーブルとの照合および自動登録処理を実行し、特定のカテゴリのアクセス要求でない場合には、アクセス制御を実行することなく、すなわち、ＭＡＣアドレステーブルとの照合および自動登録処理を実行することなくクライアントからの要求に応じる構成としてもよい。

特定のカテゴリのアクセス要求とは、例えば、サーバの保有するコンテンツの取得要求や、サーバに対する制御要求である。例えばＵＰｎＰ機器において、サーバの保有するコンテンツの取得要求は、コンテンツの識別子としてのコンテンツＵＲＬ（Uniform Resource Locators）を指定したＨＴＴＰ(Hyper Text Transfer Protocol)ＧＥＴメソッドに基づいて実行される。また、サーバに対する制御要求はＳＯＡＰ（Simple Object Access Protocol）プロトコルが利用される。

アクセス制御を行なうネットワーク接続機器としての情報処理装置（サーバ）が（１）自動登録アクセス制御モードにある場合、クライアントからの要求が、コンテンツＵＲＬ（Uniform Resource Locators）を指定したＨＴＴＰ(Hyper Text Transfer Protocol)ＧＥＴメソッドであるか、あるいは、ＳＯＡＰ（Simple Object Access Protocol）プロトコルに基づくサーバに対する制御要求である場合にのみ、アクセス制御処理としてのＭＡＣアドレステーブルとの照合および自動登録処理を実行し、ＭＡＣアドレステーブルに登録済みであることを条件としてアクセス要求を許容する。クライアントからのアクセスがＨＴＴＰ－ＧＥＴメソッドに基づくコンテンツ取得要求、あるいはＳＯＡＰに基づく制御要求以外、例えば、ＵＰｎＰにおける機器発見処理としてのディスカバリ要求である場合などには、アクセス制御処理としてのＭＡＣアドレステーブルとの照合および自動登録処理を実行することなく、無条件にクライアントの要求を受領し、応答を実行する。

サーバにおいて、クライアントからの要求種別を判別して、アクセス制御処理としてのＭＡＣアドレステーブルとの照合および自動登録処理を実行するか否かを判定して処理を実行するシーケンスについて、図６のフローチャートを参照して説明する。

図６の処理フローは、アクセス制御を行なうネットワーク接続機器としての情報処理装置（サーバ）が自動登録アクセス制御モードにある場合の処理である。

ステップＳ２０１において、アクセス制御を行なうネットワーク接続機器としての情報処理装置は、他のネットワーク接続機器からのアクセス要求を受信する。ステップＳ２０２では、クライアントからのアクセス要求が、ＨＴＴＰ－ＧＥＴメソッドに基づくコンテンツ取得要求、あるいはＳＯＡＰに基づく制御要求であるか否かを判定する。

クライアントからのアクセス要求が、ＨＴＴＰ－ＧＥＴメソッドに基づくコンテンツ取得要求、あるいはＳＯＡＰに基づく制御要求である場合（ステップＳ２０２：Ｙｅｓ）には、ステップＳ２０３において、受信パケットからアクセス要求元のＭＡＣアドレスを取得し、サーバの記憶部に格納したＭＡＣアドレステーブル(図３参照)に登録されたＭＡＣアドレスとの照合処理を実行し、登録済みか否かを判定する。登録済みである場合（ステップＳ２０３：Ｙｅｓ）は、ステップＳ２０６に進み、アクセスを許可し、クライアントの要求に応じた処理を実行する。

登録済みでない場合（ステップＳ２０３：Ｎｏ）は、ステップＳ２０４に進み、ＭＡＣアドレステーブルにすでに登録されたＭＡＣアドレスがサーバに設定した登録限度数：Ｎに達していないか、すなわち、登録ＭＡＣアドレス＜登録限度数：Ｎであるか否かを判定する。

登録ＭＡＣアドレス＜登録限度数：Ｎである場合（ステップＳ２０４：Ｙｅｓ）は、ステップＳ２０５において、クライアントからの受信パケットのヘッダ部に設定されている送信元ＭＡＣアドレスをＭＡＣアドレステーブルに登録し、その後、ステップＳ２０６においてアクセスを許可し、クライアントの要求に応じた処理を実行する。

登録ＭＡＣアドレス＜登録限度数：Ｎでない場合（ステップＳ２０４：Ｎｏ）、すなわち、ＭＡＣアドレステーブルに既に登録限度数：ＮのＭＡＣアドレスが登録済みである場合は、これ以上の自動登録を実行できないので、ＭＡＣアドレスの登録処理を実行することなく、ステップＳ２０７において、クライアントからのアクセス要求を拒絶する。

一方、ステップＳ２０２において、クライアントからのアクセス要求が、ＨＴＴＰ－ＧＥＴメソッドに基づくコンテンツ取得要求、あるいはＳＯＡＰに基づく制御要求でないと判定した場合には、ＭＡＣアドレステーブルとの照合、

自動登録処理を実行することなく、ステップＳ２０６に進み、アクセスを許可し、クライアントの要求に応じた処理を実行する。

図７に、アクセス制御を実行するネットワーク接続機器（サーバ）のアクセス制御処理を説明する機能ブロック図を示す。サーバは、ネットワークを介したパケットの送受信を実行するパケット送受信部５０１、パケット送受信部５０１を介して受信するパケットの解析および、パケット送受信部５０１を介して送信するパケットを生成するパケット生成、解析部５０２、クライアントから受信するパケットに基づいてＭＡＣアドレステーブルに対する登録可否を判定し、登録可と判定した場合にＭＡＣアドレスの登録処理を実行する登録処理実行部５０３、ＭＡＣアドレステーブルを格納した記憶部５０４、さらに、サーバに対する様々なデータ処理要求パケットに基づいて、データ処理要求クライアントがＭＡＣアドレステーブルに登録されているか否か等を判断し、アクセス可否判定処理を実行するアクセス制御処理実行部５０５、アクセス制御処理実行部５０５におけるアクセス可の判定を条件として、クライアントの要求するデータ処理を実行するデータ処理部５０７、サーバが（１）自動登録アクセス制御モードにあるか、（２）登録デバイスアクセス制御モードにあるかのモード情報を記憶したモード情報記憶部５０６を有する。

登録処理実行部５０３、アクセス制御処理実行部５０５は、モード情報記憶部５０６に設定されたモード設定情報、すなわち、（１）自動登録アクセス制御モード、（２）登録デバイスアクセス制御モードの２つのモードのいずれのモードにあるかに応じて異なる処理を実行する。例えば、（１）自動登録アクセス制御モードにある場合は、登録処理実行部５０３は、記憶部５０４に記憶されたＭＡＣアドレステーブルの登録エントリ数に基づいて、自動登録が許容されるか否かの判定を実行し、限度数以内であることを条件とした登録処理を実行する。

また、登録処理実行部５０３は、マニュアル登録処理実行時における登録可

否判定処理も実行する。すなわち予め決められたマニュアル登録処理シーケンスに応じた処理が実行されているか否かを判定する処理などを実行する。なお、マニュアル登録処理の詳細例については後述する。

図８にアクセス制御を実行するネットワーク接続機器（サーバ）においてディスプレイに表示されるＭＡＣアドレステーブルおよびモード設定処理を実行するためのユーザインタフェースの例を示す。

サーバのディスプレイ６５０には、クライアント機器名、ＭＡＣアドレス、マニュアル登録か否かを示すデータからなるＭＡＣアドレステーブル６５１が表示され、さらに、現在の設定モード情報表示部６５２、モード切り替え部６５４とマニュアル登録処理においてＭＡＣアドレスを登録する際の登録確認ボタン６５５を持つユーザ入力部６５３、さらにＭＡＣアドレステーブル６５１に登録されたエントリを削除するための削除ボタン６５６を持つユーザインタフェース（ＵＩ）が表示される。

クライアントからのアクセス要求である、すべてのＨＴＴＰ－ＧＥＴメソッドおよびＳＯＡＰには、図９のような送信者の情報を示すＨＴＴＰ拡張ヘッダ（Ｘ－ＡＶ－Ｃｌｉｅｎｔ－Ｉｎｆｏ）が付加されており、ディスプレイ６５０には、この情報に基づく表示処理がなされる。すなわち、例えば、図９に示すように、

```
GET /tracks/track?id=254 HTTP/1.1 ¥r¥n
Host:192.254.32.11:80 ¥r¥n
X-AV-Client-Info: av=2.0 ; cn ="Sony Corporation" ;mn=Linux-Sample-CP ;
mv=2002-11-22-2.0 ¥r¥n
```

からなるＨＴＴＰ拡張ヘッダ（Ｘ－ＡＶ－Ｃｌｉｅｎｔ－Ｉｎｆｏ）がクライアントから送信される。

ユーザは、図８に示すようなＵＩをサーバのディスプレイに表示し、モード

の切り替えを実行し、また、ＭＡＣアドレステーブルに登録されたＭＡＣアドレスの確認を実行することができ、さらに、必要に応じてＭＡＣアドレステーブルに登録されたＭＡＣアドレスの削除処理を実行する。

［マニュアル登録処理］

次に、アクセス制御を実行する情報処理装置が実行するＭＡＣアドレスのマニュアル登録処理の手順について、図１０のシーケンス図を参照して説明する。なお、図１０に示す例は、マニュアルによるＭＡＣアドレス登録処理の一例であり、必ずしもこの例に従ったマニュアル登録を行うことが必須ではない。ただし、あらかじめ定められたマニュアル登録を行ったクライアントのＭＡＣアドレスのみが、図３に示すＭＡＣアドレステーブル（ＭＡＣリスト）にマニュアル登録されたＭＡＣアドレスとしてエントリが設定される。

図１０に示すシーケンスは、パスワードを用いた機器認証に基づくＭＡＣ登録処理シーケンスである。まず、ステップＳ３０１において、ユーザがクライアント（コントローラ）側に設けられた登録ボタンを押下する。すると、クライアント装置は登録ボタンの押下に応じて発生するユーザシグナルＡ（ＵＳＡ）に従い、ステップＳ３０２において、ＭＡＣアドレス登録要求をネットワークを介してブロードキャスト送信する。ＭＡＣアドレス登録要求のブロードキャスト送信は、例えば３秒毎に数分間継続して実行される。

クライアント（コントローラ）側に設けられた登録ボタンを押下した後、ユーザはサーバ（デバイス）側に移動する。そして、ステップＳ３０３において、サーバ側に設けられた確認ボタンを押下する。すると、サーバは確認ボタンの押下に応じて発生するユーザシグナルＢ（ＵＳＢ）に従い、ステップＳ３０４において、ＭＡＣアドレス登録要求を規定時間、例えば１０秒間受信する。

１０秒間に同一の送信元（ＭＡＣアドレス）からＭＡＣアドレス登録要求を受信した場合、サーバはそのＭＡＣアドレスをＭＡＣアドレステーブル（ＭＡ

Cリスト）（図３参照）に仮記憶した後、ユーザに対して「機器を発見しました。登録しますか？」なるメッセージを表示するデバイスシグナルA（ＤＳＡ）を発生（Ｓ３０５）し、その状態で所定時間（たとえば１分間）待機する。

なお、サーバは、ＭＡＣアドレステーブルを参照し、既にマニュアル登録済みのクライアントからのＭＡＣアドレス登録要求であると判定した場合、ＭＡＣ登録完了を意味する通知をクライアントに送信してＭＡＣアドレス登録処理を終了する。すなわちサーバは同一のＭＡＣアドレスの二重登録は行わない。

ただし、マニュアル登録されていないが、自動登録処理によってＭＡＣアドレステーブルに登録されているＭＡＣアドレスと一致するＭＡＣアドレスのマニュアル登録処理である場合は、サーバは、ＭＡＣアドレステーブルに登録されているＭＡＣアドレスデータエントリを自動登録エントリからマニュアル登録エントリへ変更する処理を行う。

この変更処理においては、サーバは、ＭＡＣアドレステーブルの自動登録処理のなされたＭＡＣアドレスデータのエントリに対応するマニュアル登録フィールドにマニュアル登録がなされたことを示す識別子を設定する処理を実行することになる。

サーバが、ステップＳ３０５において、「機器を発見しました。登録しますか？」なるメッセージを表示するデバイスシグナルA（ＤＳＡ）を発生した状態で所定時間(例えば１分間)待機している間に、ステップＳ３０６において、ユーザがサーバ側に設けられた確認ボタン（図８の登録確認ボタン６５５）を押下する。すると、サーバは確認ボタンの押下に応じて発生するユーザシグナルC（ＵＳＣ）に従い、ステップＳ３０７において、ＭＡＣ登録確認要求をクライアントに対して送信する。ＭＡＣ登録確認要求には、パスワード要求フラグが付加される。

クライアントは、パスワード要求フラグが付加されたＭＡＣ登録確認要求をサーバから受信すると、ステップＳ３０８において、受信したＭＡＣ登録確認要求に含まれるパスワード要求フラグに基づき、ユーザに対して「デバイス“ＸＸＸ”のパスワードを入力してください。」なるメッセージを表示するデバイスシグナルＢ（ＤＳＢ）を発生し、パスワードの入力を所定時間（例えば５分間）待機する。

さらに、クライアントは、ＭＡＣアドレス登録要求の送信を停止し、ステップＳ３０９において、サーバへＭＡＣ登録確認レスポンスを返信する。

サーバは、このＭＡＣ登録確認レスポンスを受信すると、ステップＳ３１０において、パスワード（ワンタイムパスワード）を生成し、ユーザに対して「クライアント（コントローラ）“ＹＹＹＹ”のためのパスワードは”○○○○”です。」なるメッセージを表示するデバイスシグナルＣ（ＤＳＣ）を発生し、パスワードを提示した状態で規定時間（例えば５分間）待機する。

一方、クライアント側では、パスワードの入力待機中に、ステップＳ３１１で、ユーザがパスワードを入力すると、ステップＳ３１２で、クライアントから入力パスワードがサーバに送信される。

サーバは、パスワードをクライアントから受信すると、ステップＳ３１０で生成しサーバ側でユーザに対して提示したパスワードと、受信パスワードとの照合処理を実行する。クライアントからの受信パスワードと生成パスワードとが一致すると、ステップＳ３１３において、サーバはＭＡＣアドレステーブル（ＭＡＣリスト）（図３参照）にクライアントのＭＡＣアドレスを正式エントリとして設定するとともに、マニュアル登録であることを示す識別データ（フラグなど）を設定する。または自動登録エントリをマニュアル登録エントリに変更する。

サーバはＭＡＣアドレスの登録が済むと、ステップＳ３１４において、ユーザに対して「クライアント（コントローラ）“ＹＹＹＹ”を登録しました。」なるメッセージを表示するデバイスシグナルＤ（ＤＳＤ）を発生し、ステップＳ３１５において、クライアントに照合ＯＫを付加したパスワードレスポンスを返信する。

クライアントは、サーバからパスワード照合ＯＫに基づくＭＡＣアドレス登録通知としてのパスワードレスポンスを受信すると、ステップＳ３１６において、ＭＡＣアドレスが認証登録されたとして、ユーザに対して「デバイス“ＸＸＸ”に登録されました。」なるメッセージを表示するデバイスシグナルＥ（ＤＳＥ）を発生してＭＡＣアドレスの機器認証を伴うマニュアル登録処理を終える。

なお、クライアントから送られてきたパスワードが不正、すなわちクライアントからの受信パスワードとサーバの生成パスワードが不一致であると、サーバはクライアントに照合ＮＧを付加したパスワードレスポンスを返信し、クライアントから再度パスワード入力されるのを待機し、待機期間中にパスワード照合ＮＧが３回連続すると、サーバはパスワード入力の再試行を中止させ、ユーザに対して「コントローラ“ＹＹＹＹ”を登録できません。」なるメッセージを表示し、クライアントのＭＡＣアドレス登録を実行することなく処理を終了する。

上述したＭＡＣアドレスのマニュアル登録処理を実行したクライアントのＭＡＣアドレスのみが、ＭＡＣアドレステーブルにマニュアル登録ＭＡＣアドレスとして登録されることになる。

サーバが「登録デバイスアクセス制御モード」にある場合は、これらのマニュアル登録されたクライアントのみが、アクセスを許容されることになる。

[サーバおよびクライアントの機能構成]

サーバおよびクライアント装置のハードウェア構成については、先に図２を参照して説明した通りであり、上述した各種の処理は、サーバクライアントそれぞれの記憶部に格納されたプログラムに従って制御部としてのＣＰＵが実行する。

ＣＰＵによって実行される処理は、例えばサーバ側では、クライアントからの要求を入力し、入力情報の解析、解析結果に基づくＭＡＣアドレステーブル（ＭＡＣリスト）、すなわちアクセス制御情報へ登録する処理、クライアントと送受信するパケット生成、解析処理、さらに、登録処理における各種メッセージ出力、ユーザ入力情報の解析処理等である。クライアント側の処理としては、サーバに対する各種要求パケットの生成、送信、サーバから受信するパケット解析処理、さらに、登録処理における各種メッセージ出力、ユーザ入力情報の解析処理等である

基本的にこれらの処理は、サーバ、クライアント装置の制御部としてのＣＰＵの制御の下に予め格納された処理プログラムに従って実行される。制御部としてのＣＰＵが実行する処理および記憶部の格納データ等について、図１１および図１２を参照して説明する。図１１は、サーバの主要機能構成を説明するブロック図であり、図１２は、クライアントの主要機能構成を説明するブロック図である。

まず、図１１のサーバの機能構成を示すブロック図を参照してサーバの機能構成について説明する。パケット送受信部７０１は、クライアントに対するパケット、クライアントからのパケットを受信する。パケット生成、解析部７０２は、送信パケットの生成処理、受信パケットの解析処理を行う。パケットのアドレス設定、アドレス認識、パケットのデータ格納部に対するデータ格納、データ格納部からのデータ取得処理などである。

データ入力部７０３は、ユーザによるデータ入力を実行するためのキーボード、ユーザインタフェースなどである。データ出力部７０４は、メッセージデータ等を表示するディスプレイ等の出力部である。

アクセス制御処理実行部７０５は、先に図４、図６を参照して説明した（１）自動登録アクセス制御モードにおけるアクセス制御処理、（２）登録デバイスアクセス制御モードにおけるアクセス制御処理を実行する。

登録処理部７０６は、（１）自動登録アクセス制御モードにおけるアクセスに対応して実行するＭＡＣアドレス登録処理と、先に図１０を参照して説明したマニュアル登録処理を実行する。すなわち、登録処理部７０６は、例えば、図１０を参照して説明したマニュアル登録処理のように、予め規定されたＭＡＣアドレス登録処理シーケンスに従った処理が実行されたことを条件として、クライアントＭＡＣアドレスをＭＡＣアドレステーブルにマニュアル登録ＭＡＣアドレスとして登録する処理を実行する。

さらに、登録処理部７０６は、予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたＭＡＣアドレスが、自動登録ＭＡＣアドレスとしてテーブルに登録されている場合は、自動登録クライアントＭＡＣアドレスエントリをマニュアル登録クライアントＭＡＣアドレスエントリとする設定変更処理を実行する。

データ処理部７０７は、アクセスの許可されたクライアントからの要求、例えばコンテンツ取得処理等に対応する処理を実行する。記憶部７０８には、アクセス制御処理実行部７０５において実行するアクセス制御処理プログラム７１１、登録処理部７０６において実行するＭＡＣアドレス登録処理プログラム７１２等の各種データ処理プログラムが格納され、さらに、図３を参照して説明したＭＡＣアドレステーブル７１３、さらにサーバに設定されたモード情報７１４が格納される。なお、サーバはさらにクライアントに提供するコンテ

ンツ、コンテンツに対応するメタデータ等を格納している。

次に、クライアント装置の機能構成について、図１２を参照して説明する。パケット送受信部８０１は、サーバに対するパケット、サーバからのパケットを受信する。パケット生成、解析部８０２は、送信パケットの生成処理、受信パケットの解析処理を行う。パケットのアドレス設定、アドレス認識、パケットのデータ格納部に対するデータ格納、データ格納部からのデータ取得処理などである。

データ入力部８０３は、ユーザによるデータ入力を実行するためのキーボード、ユーザインタフェースなどである。データ出力部８０４は、メッセージデータ等を表示するディスプレイ等の出力部である。

アクセス要求処理実行部８０５は、コンテンツ取得要求、制御要求等のサーバに対する各種のアクセス要求処理を実行する。アドレス登録処理実行部８０６は、図１０を参照して説明したＭＡＣアドレスのマニュアル登録処理を実行する。

データ処理部は、サーバから取得したコンテンツの再生処理など、様々なデータ処理を実行する。記憶部８０８には、アドレス登録処理実行部８０６において実行するアドレス登録処理プログラム８１１他の処理プログラム、さらにクライアントのＭＡＣアドレス８１２などが格納される。

サーバ、およびクライアントは、機能的には図１１、図１２に示す各機能を有し、上述した各処理を実行する。ただし、図１１、図１２に示すブロック図は、機能を説明するブロック図であり、サーバクライアントが図１１、図１２に示すブロックに対応するハードウェアを有することは必須ではない。具体的には、図２に示すＰＣ等の構成におけるＣＰＵの制御の下に各種の処理プログラムが実行され、図１１、図１２に示す各ブロックを参照して説明した処理、

あるいは上述の発明の詳細な説明において説明した各処理が実行される。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ(Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

産業上の利用可能性

以上、説明したように、本発明の構成においては、マニュアル登録のなされたクライアントＭＡＣアドレスと、自動登録処理のなされたクライアントＭＡＣアドレスとを識別可能な態様で登録したＭＡＣアドレステーブルを設定し、アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスを、ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスが、ＭＡＣアドレステーブルに、マニュアル登録されたＭＡＣアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行する構成としたので、ユーザによるマニュアル登録処理を実行しない場合においても、無制限なアクセスが防止され、例えば不特定多数クライアントからのサーバ格納コンテンツの取得等を防止することが可能となり、さらに、モードを、登録デバイスアクセス制御モードに設定することにより、厳格なアクセス制御を実行することも可能となる。

さらに、本発明の構成によれば、自動登録アクセス制御モードにおいて、クライアントのアクセス要求種別を識別し、識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別、例えばＨＴＴＰ（Hyper Text Transfer Protocol）－ＧＥＴメソッドに基づくコンテンツ要求処理、またはＳ

ＯＡＰ（Simple Object Access Protocol）に基づく制御要求処理である場合にのみ、クライアントのＭＡＣアドレスを、ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としたアクセス許容を実行する構成としたので、ＵＰｎＰ等における機器発見処理、情報取得処理等において不必要なアクセス制御を行うことが防止される。

請求の範囲

1．アクセス制御処理を実行する情報処理装置であり、

マニュアル登録のなされたクライアントＭＡＣアドレスと、自動登録処理のなされたクライアントＭＡＣアドレスとを識別可能な態様で登録したＭＡＣアドレステーブルを記憶した記憶部と、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかに応じて、クライアントからのアクセス要求に対して異なるアクセス制御処理を実行するアクセス制御部とを有し、

前記アクセス制御部は、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスを、前記ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

情報処理装置に設定されたアクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスが、前記ＭＡＣアドレステーブルに、マニュアル登録されたＭＡＣアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行する構成を有することを特徴とする情報処理装置。

2．前記アクセス制御部は、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合、クライアントのアクセス要求種別を識別し、該識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別である場合にのみ、クライアントのＭＡＣアドレスを、前記ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容する処理を実行する構成であることを特徴とする請求項１に

記載の情報処理装置。

３．前記アクセス制御を実行すべき要求種別は、

ＨＴＴＰ(Hyper Text Transfer Protocol)－ＧＥＴメソッドに基づくコンテンツ要求処理、またはＳＯＡＰ（Simple Object Access Protocol）に基づく制御要求処理の少なくともいずれかを含むことを特徴とする請求項２に記載の情報処理装置。

４．前記情報処理装置は、

予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、クライアントＭＡＣアドレスを前記ＭＡＣアドレステーブルにマニュアル登録のなされたクライアントＭＡＣアドレスとして登録する処理を実行する登録処理部を有することを特徴とする請求項１に記載の情報処理装置。

５．前記情報処理装置は、

前記ＭＡＣアドレステーブルに自動登録のなされたクライアントＭＡＣアドレスとして登録されたＭＡＣアドレスについて、予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、前記ＭＡＣアドレステーブルの自動登録クライアントＭＡＣアドレスエントリをマニュアル登録クライアントＭＡＣアドレスエントリとする設定変更処理を実行する登録処理部を有することを特徴とする請求項１に記載の情報処理装置。

６．情報処理装置におけるアクセス制御処理方法であり、

クライアントからのアクセス要求を受信するアクセス要求受信ステップと、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかを判定するモード判定ステップと、

設定アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスを、ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

設定アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスが、前記ＭＡＣアドレステーブルに、マニュアル登録されたＭＡＣアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行するアクセス制御ステップと、

を有することを特徴とするアクセス制御処理方法。

７．前記アクセス制御ステップは、

情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードである場合、クライアントのアクセス要求種別を識別し、該識別されたアクセス要求種別が予め定めたアクセス制御を実行すべき要求種別である場合にのみ、クライアントのＭＡＣアドレスを、前記ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容する処理を実行することを特徴とする請求項６に記載のアクセス制御処理方法。

８．前記アクセス制御を実行すべき要求種別は、

ＨＴＴＰ(Hyper Text Transfer Protocol)－ＧＥＴメソッドに基づくコンテンツ要求処理、またはＳＯＡＰ（Simple Object Access Protocol）に基づく制御要求処理の少なくともいずれかを含むことを特徴とする請求項７に記載のアクセス制御処理方法。

９．前記アクセス制御処理方法は、さらに、

予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、クライアントＭＡＣアドレスを前記Ｍ

ＡＣアドレステーブルにマニュアル登録のなされたクライアントＭＡＣアドレスとして登録する処理を実行する登録処理ステップを有することを特徴とする請求項６に記載のアクセス制御処理方法。

１０．前記アクセス制御処理方法は、さらに、

前記ＭＡＣアドレステーブルに自動登録のなされたクライアントＭＡＣアドレスとして登録されたＭＡＣアドレスについて、予め規定されたＭＡＣアドレス登録処理シーケンスに従ったマニュアル登録処理が実行されたことを条件として、前記ＭＡＣアドレステーブルの自動登録クライアントＭＡＣアドレスエントリをマニュアル登録クライアントＭＡＣアドレスエントリとする設定変更処理を実行する登録処理ステップを有することを特徴とする請求項６に記載のアクセス制御処理方法。

１１．情報処理装置におけるアクセス制御処理を実行するコンピュータ・プログラムであり、

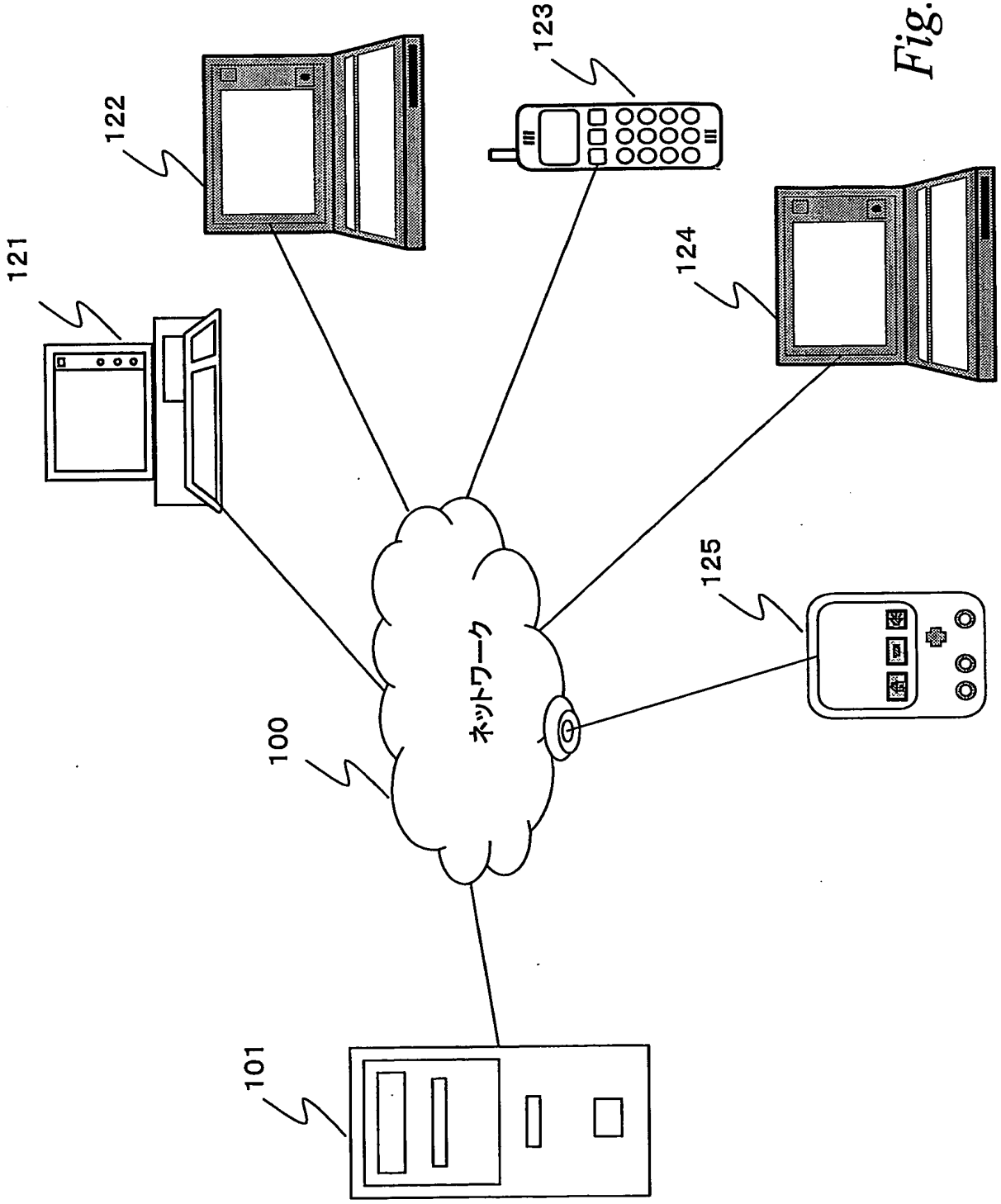
情報処理装置に設定されたアクセス制御モードが、自動登録アクセス制御モードであるか、登録デバイスアクセス制御モードであるかを判定するモード判定ステップと、

設定アクセス制御モードが、自動登録アクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスを、ＭＡＣアドレステーブルの規定登録限度数：Ｎに至るまで登録し、該登録処理を条件としてクライアントのアクセスを許容するアクセス制御処理を実行し、

設定アクセス制御モードが、登録デバイスアクセス制御モードである場合は、アクセス要求クライアントのＭＡＣアドレスが、前記ＭＡＣアドレステーブルに、マニュアル登録されたＭＡＣアドレスとして登録されていることを条件としてクライアントのアクセスを許容するアクセス制御処理を実行するアクセス制御ステップと、

を有することを特徴とするコンピュータ・プログラム。

Fig.1



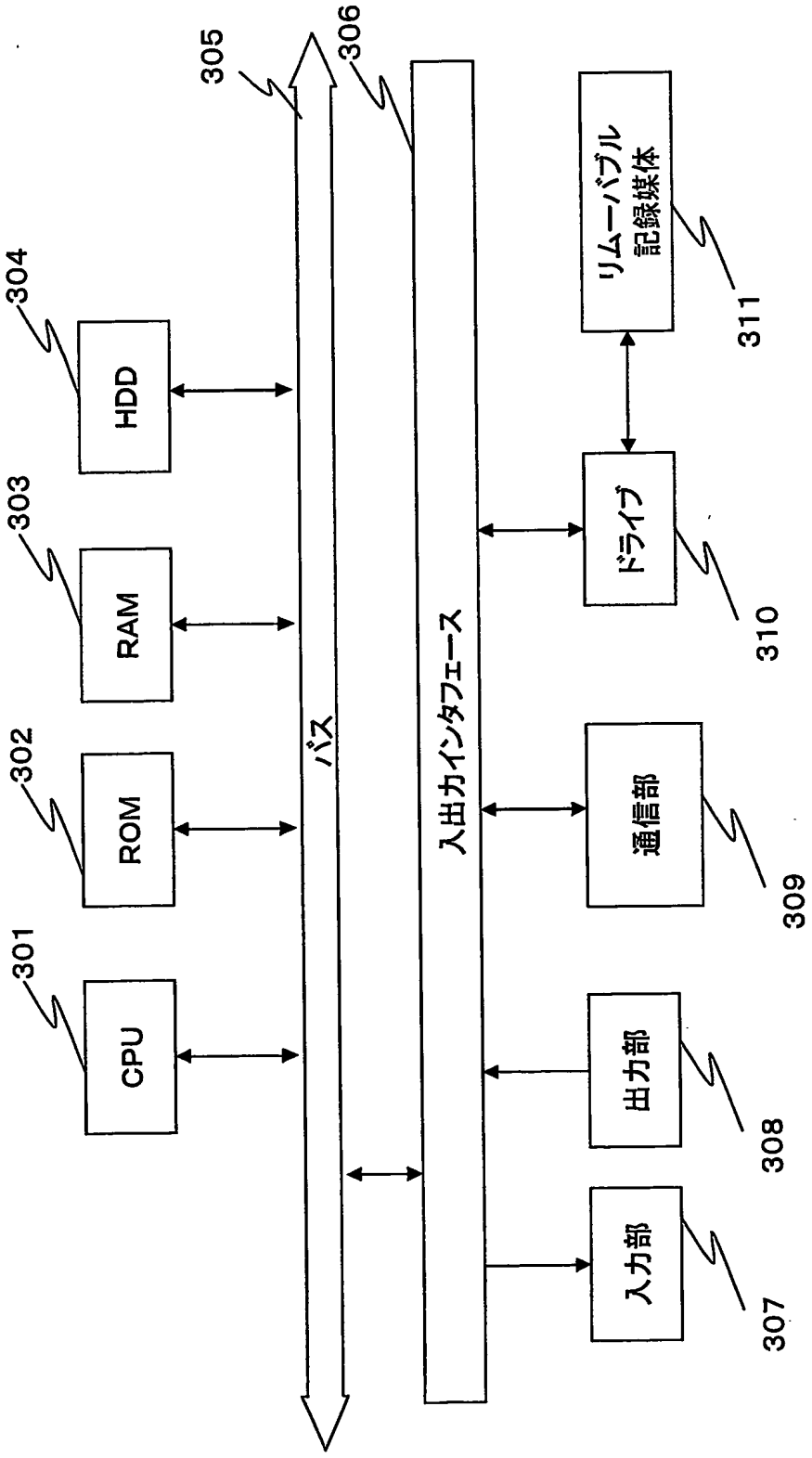

305
306
304
HDD
303
RAM
302
ROM
301
CPU
バス
入出力インタフェース
リムーバブル
記録媒体
311
ドライブ
310
通信部
309
出力部
308
入力部
307

Fig.2

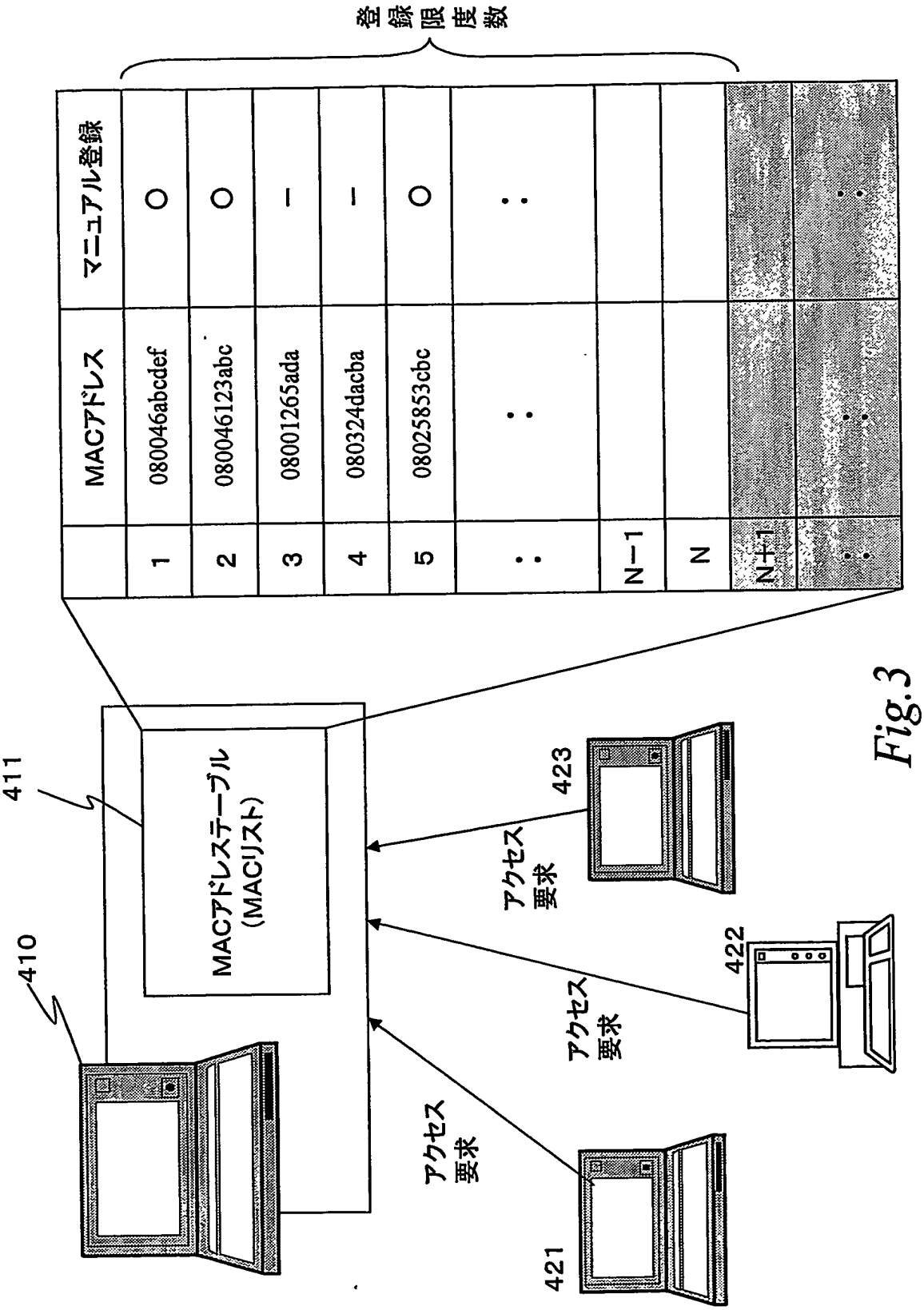

登録限度数
MACアドレス
マニュアル登録
1
080046abcdef
○
2
080046123abc
○
3
08001265ada
−
4
080324dacba
−
5
08025853cbc
○
N−1
N
N+1
411
MACアドレステーブル
(MACリスト)
410
421
422
423
アクセス
要求
アクセス
要求
アクセス
要求

Fig.3

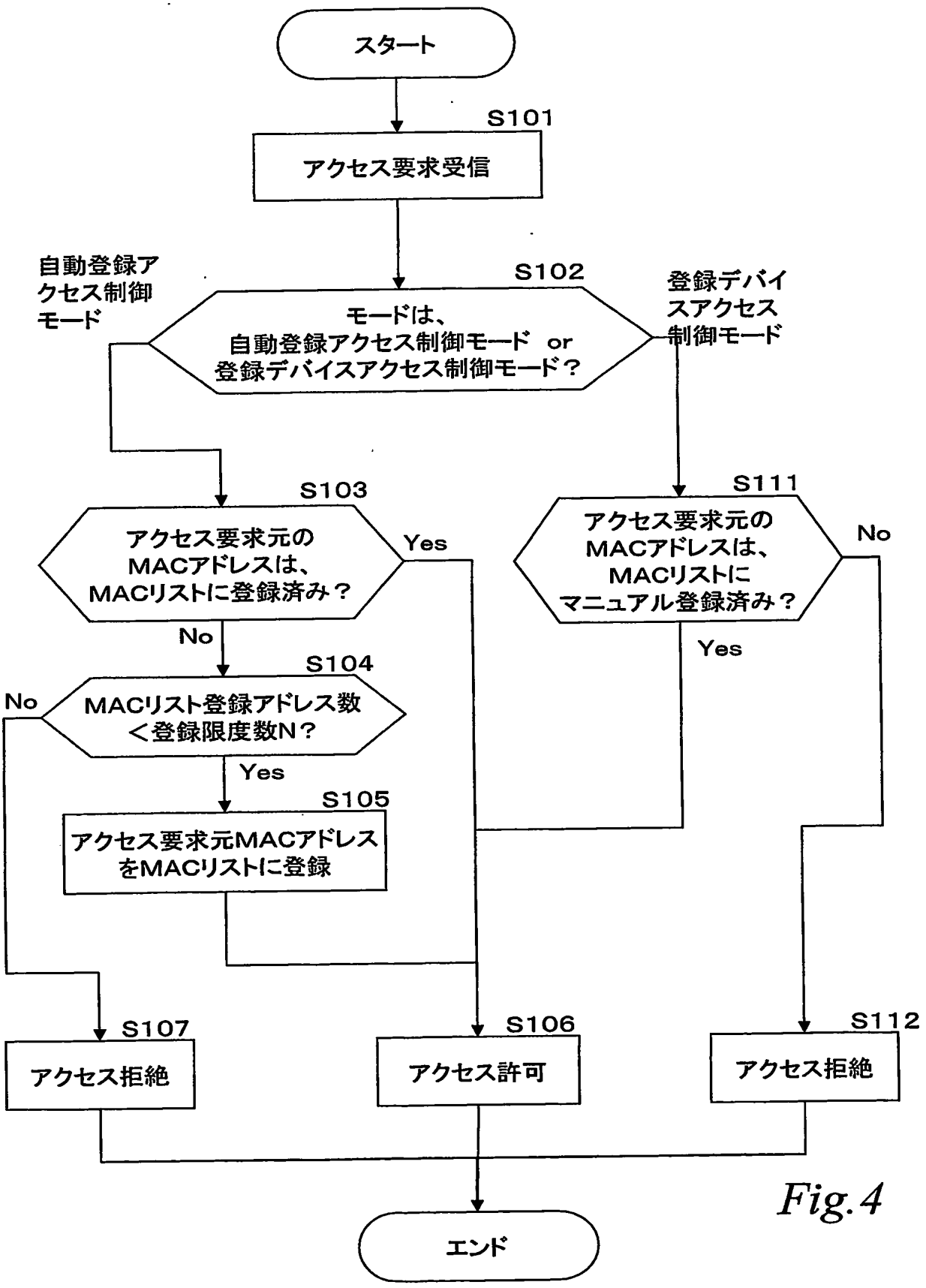

スタート
S101
アクセス要求受信
自動登録アクセス制御モード
S102
モードは、
自動登録アクセス制御モード or
登録デバイスアクセス制御モード？
登録デバイスアクセス制御モード
S103
アクセス要求元のMACアドレスは、MACリストに登録済み？
Yes
No
S111
アクセス要求元のMACアドレスは、MACリストにマニュアル登録済み？
No
Yes
S104
No
MACリスト登録アドレス数＜登録限度数N？
Yes
S105
アクセス要求元MACアドレスをMACリストに登録
S107
アクセス拒絶
S106
アクセス許可
S112
アクセス拒絶
エンド

Fig. 4

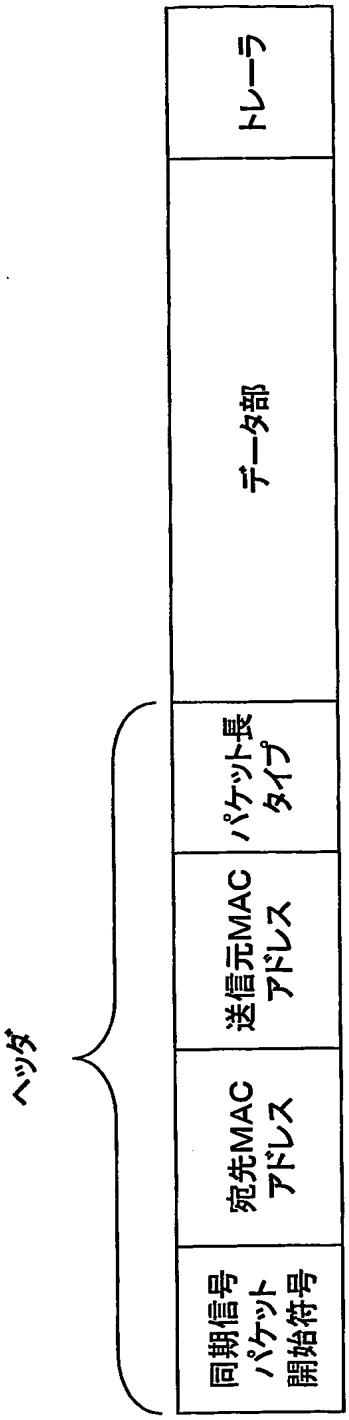

ヘッダ
同期信号
パケット
開始符号
宛先MAC
アドレス
送信元MAC
アドレス
パケット長
タイプ
データ部
トレーラ

Fig.5

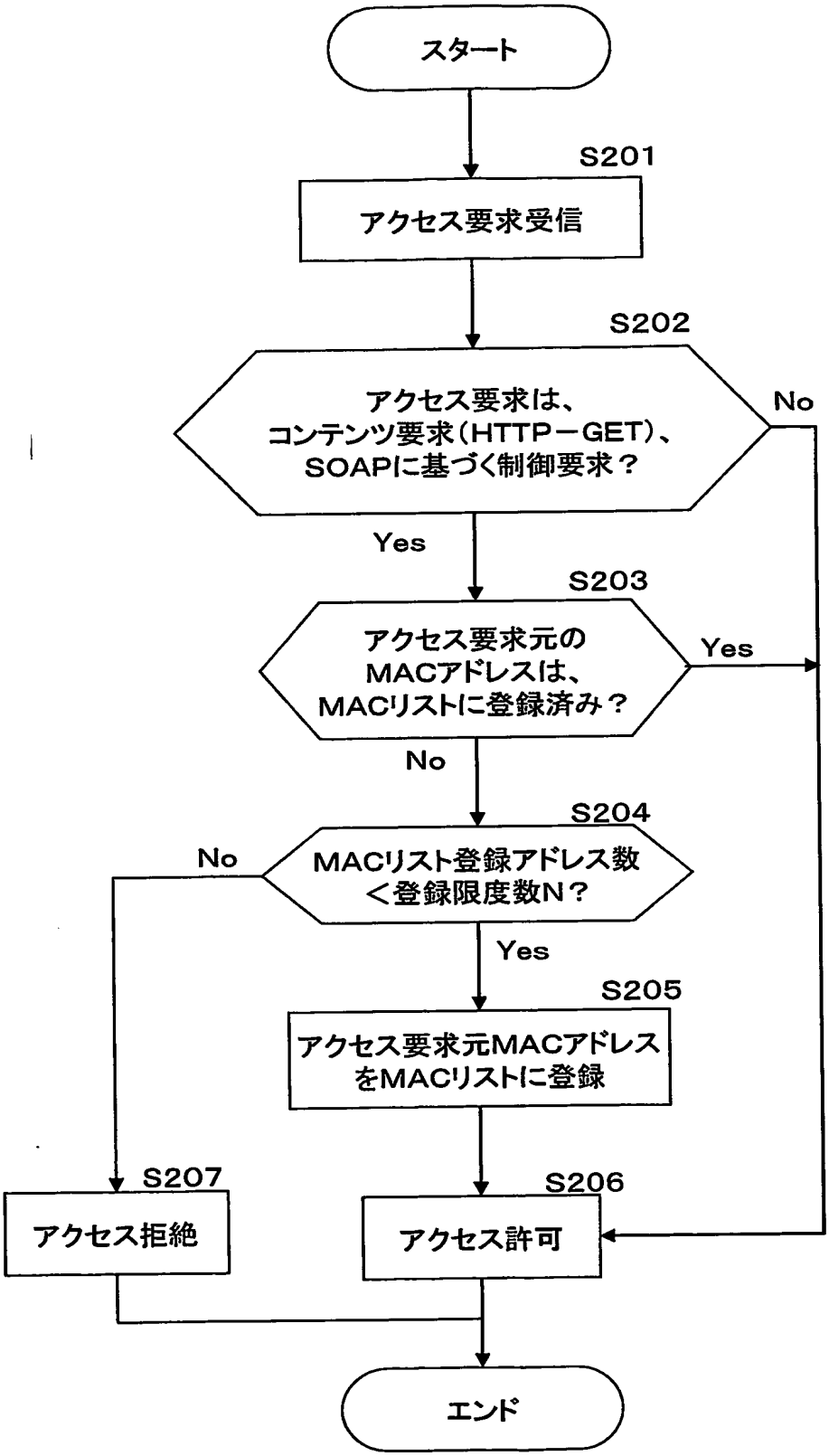

スタート
S201
アクセス要求受信
S202
アクセス要求は、
コンテンツ要求(HTTP－GET)、
SOAPに基づく制御要求？
No
Yes
S203
アクセス要求元の
MACアドレスは、
MACリストに登録済み？
Yes
No
S204
No
MACリスト登録アドレス数
＜登録限度数N？
Yes
S205
アクセス要求元MACアドレス
をMACリストに登録
S207
アクセス拒絶
S206
アクセス許可
エンド

Fig.6

Fig. 7

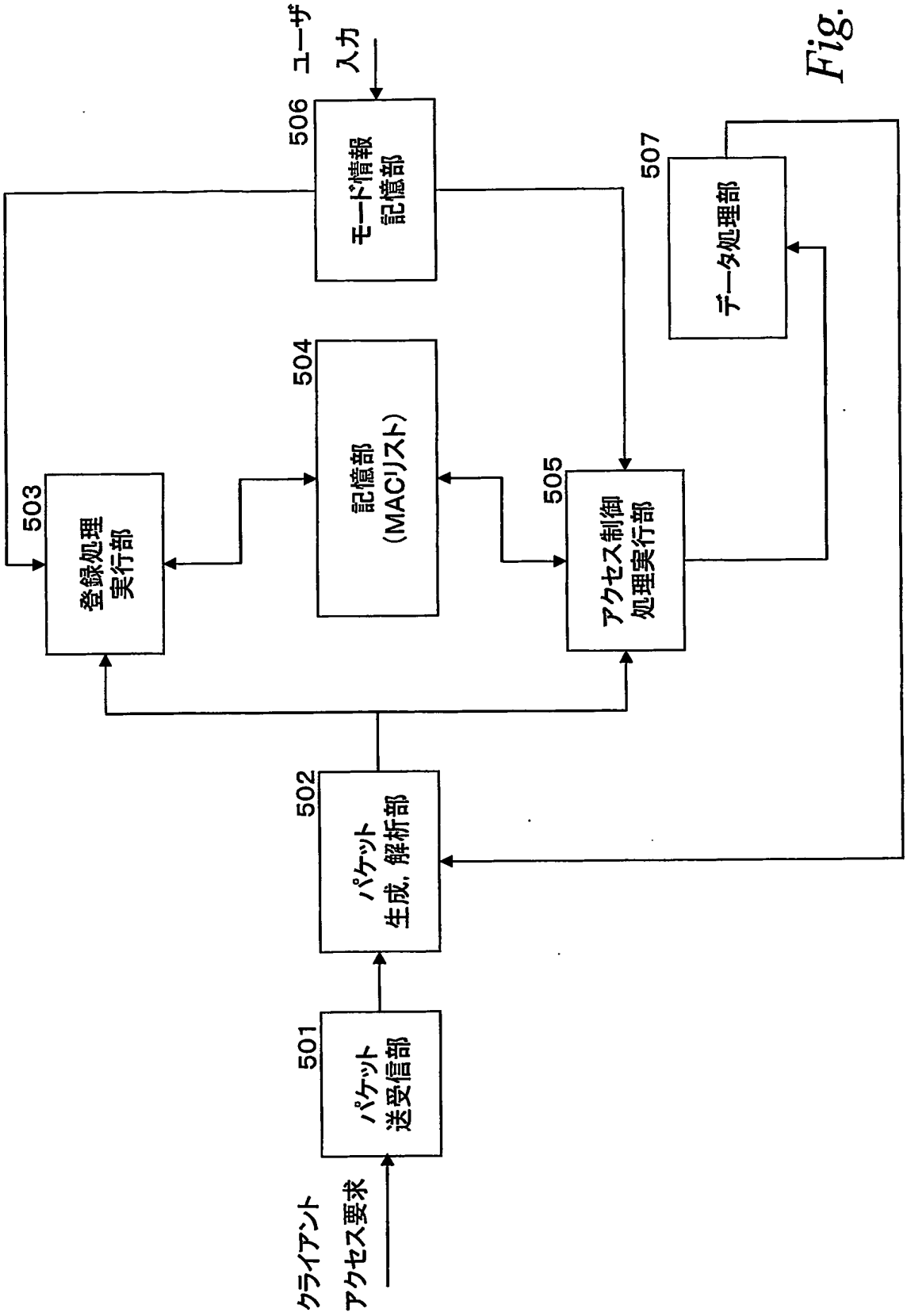
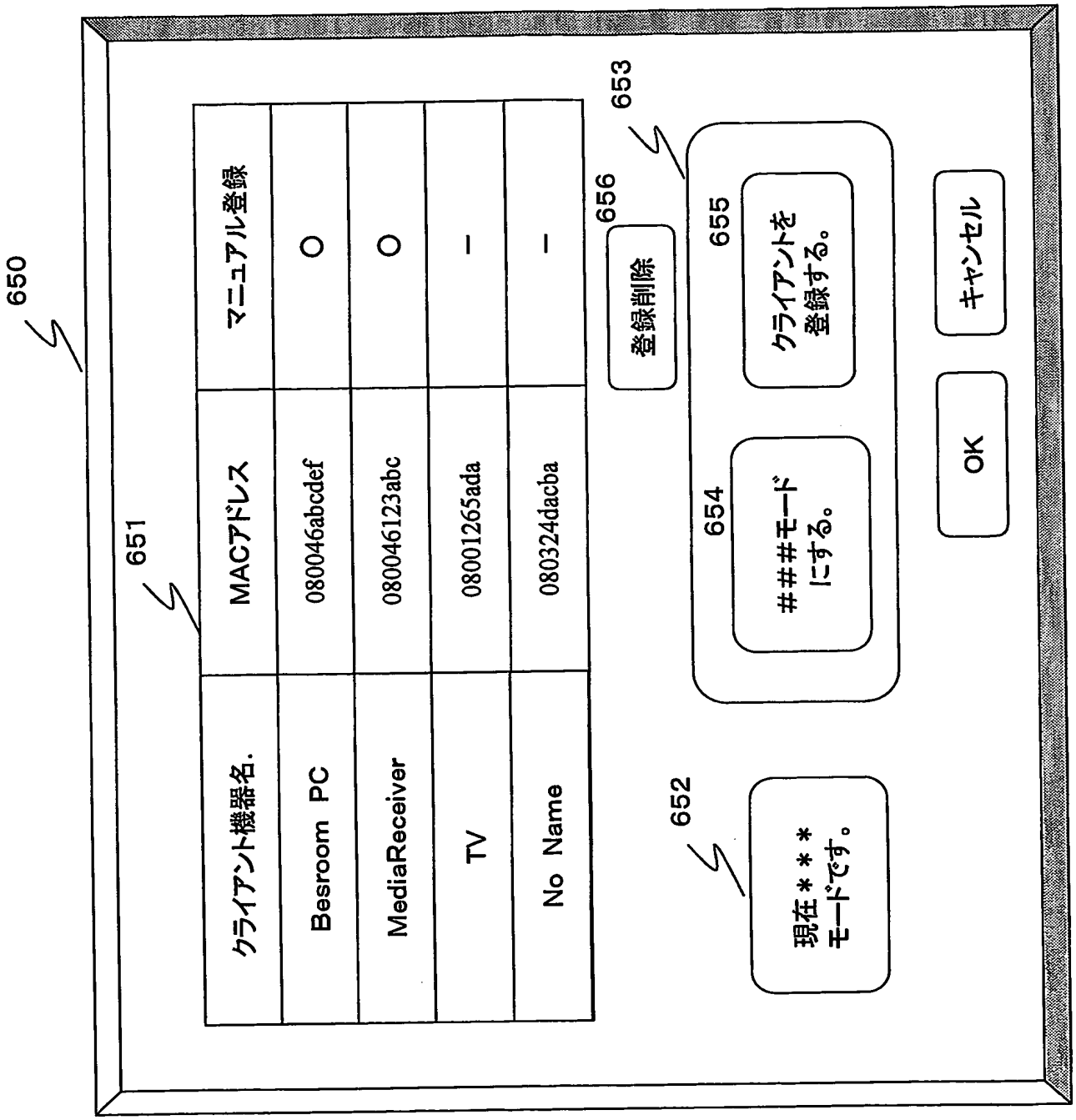

ユーザ
入力
506
モード情報
記憶部
507
データ処理部
504
記憶部
(MACリスト)
503
登録処理
実行部
505
アクセス制御
処理実行部
502
パケット
生成, 解析部
501
パケット
送受信部
クライアント
アクセス要求

Fig.8


650
651
クライアント機器名.
MACアドレス
マニュアル登録
Besroom PC
080046abcdef
○
MediaReceiver
080046123abc
○
TV
08001265ada
－
No Name
080324dacba
－
652
現在＊＊＊
モードです。
653
654
＃＃＃モード
にする。
655
クライアントを
登録する。
656
登録削除
OK
キャンセル

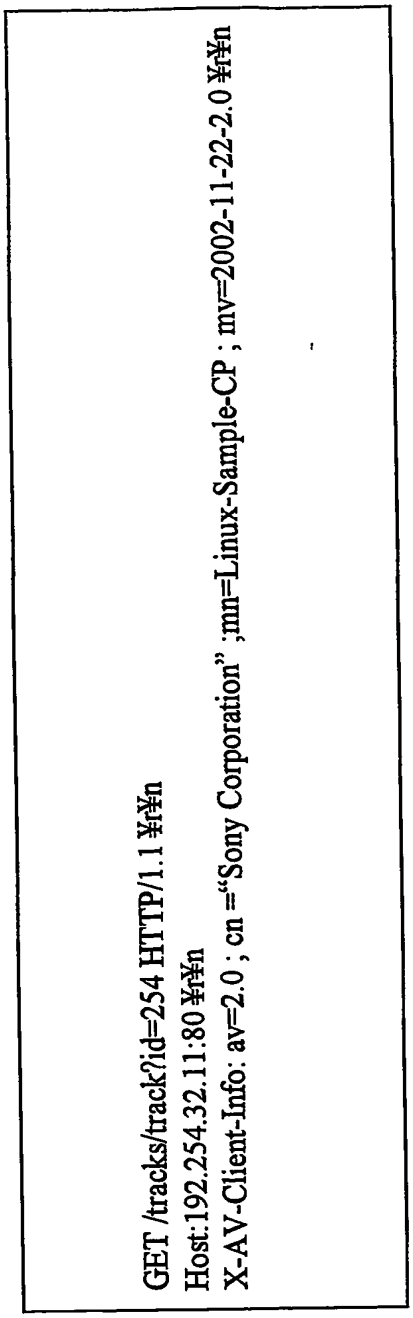

GET /tracks/track?id=254 HTTP/1.1 ¥r¥n
Host:192.254.32.11:80 ¥r¥n
X-AV-Client-Info: av=2.0 ; cn ="Sony Corporation" ;mn=Linux-Sample-CP ; mv=2002-11-22-2.0 ¥r¥n

Fig.9

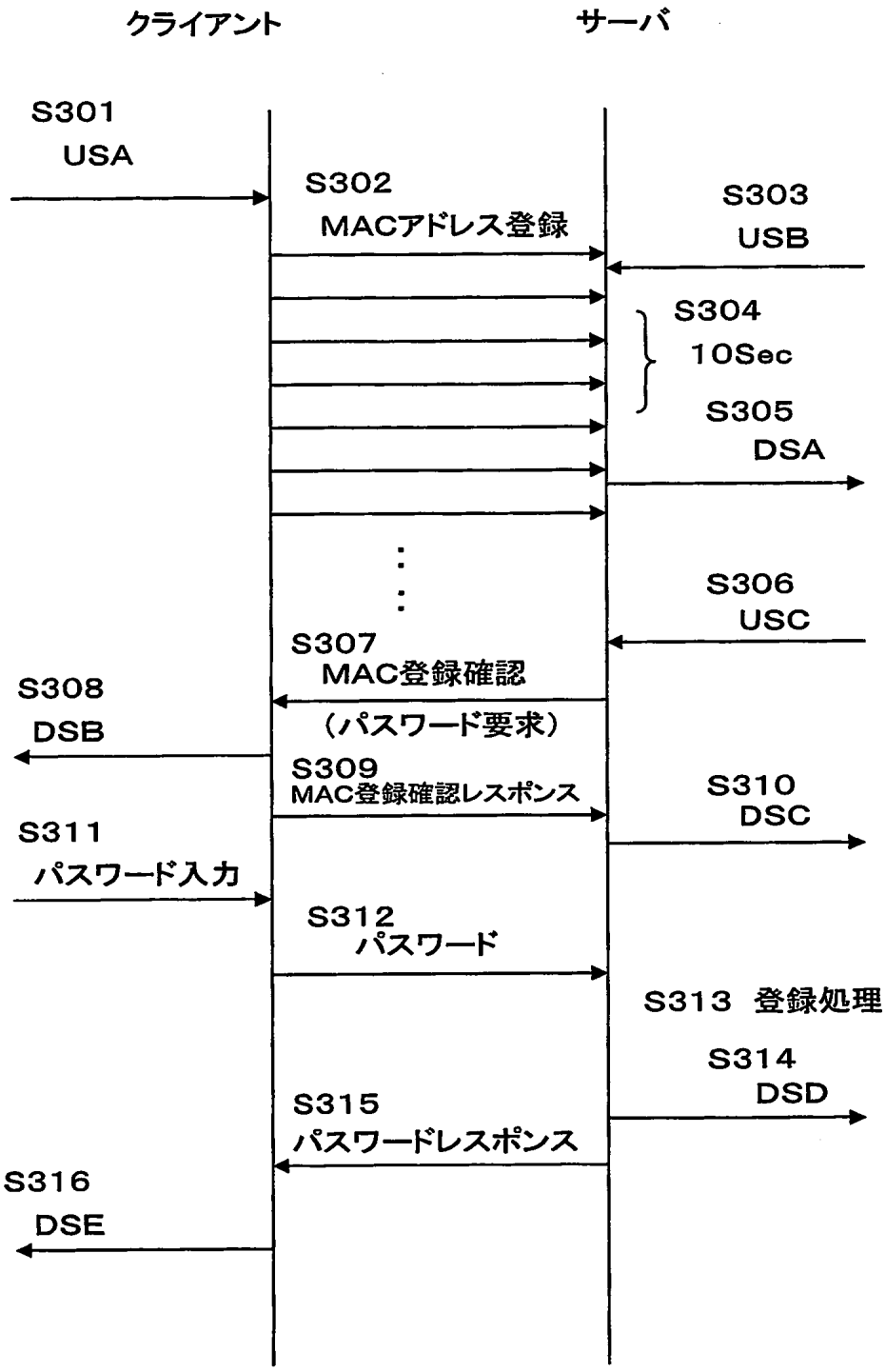

クライアント
サーバ
S301
USA
S302
MACアドレス登録
S303
USB
S304
10Sec
S305
DSA
S306
USC
S307
MAC登録確認
（パスワード要求）
S308
DSB
S309
MAC登録確認レスポンス
S310
DSC
S311
パスワード入力
S312
パスワード
S313 登録処理
S314
DSD
S315
パスワードレスポンス
S316
DSE

Fig.10

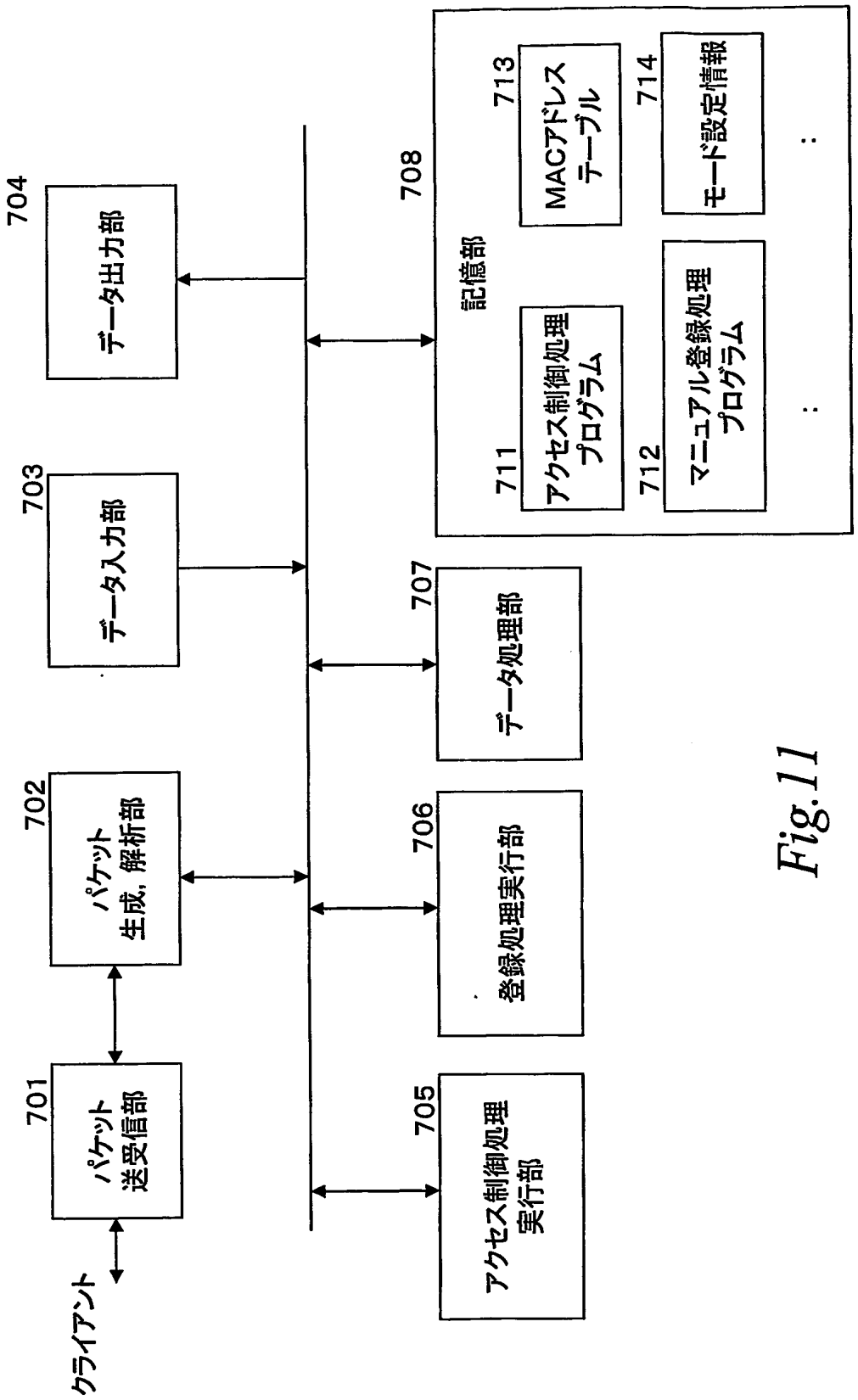

クライアント
701
パケット
送受信部
702
パケット
生成，解析部
703
データ入力部
704
データ出力部
705
アクセス制御処理
実行部
706
登録処理実行部
707
データ処理部
708
記憶部
711
アクセス制御処理
プログラム
712
マニュアル登録処理
プログラム
713
MACアドレス
テーブル
714
モード設定情報

Fig.11

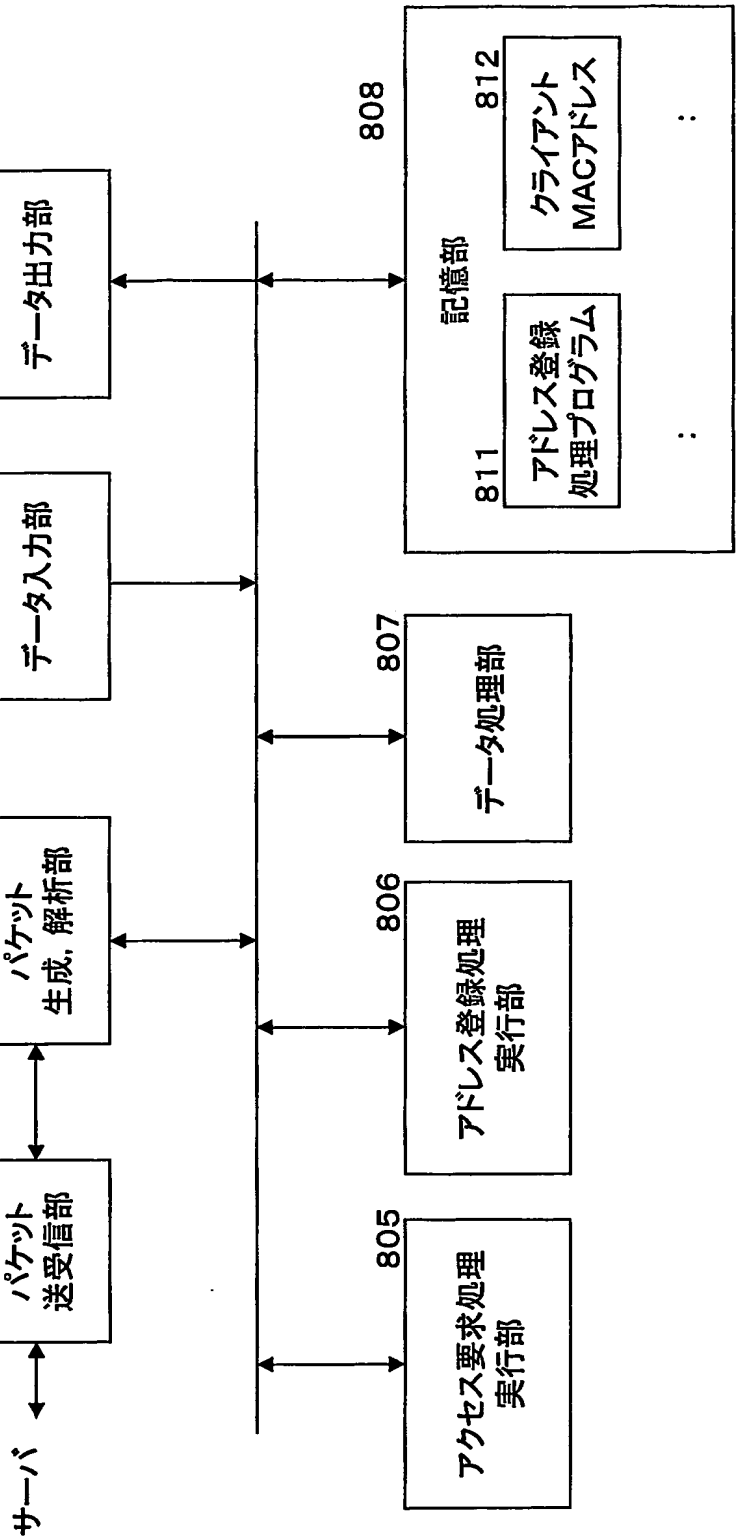

サーバ
801
パケット
送受信部
802
パケット
生成，解析部
803
データ入力部
804
データ出力部
805
アクセス要求処理
実行部
806
アドレス登録処理
実行部
807
データ処理部
808
記憶部
811
アドレス登録
処理プログラム
812
クライアント
MACアドレス

Fig.12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/004919

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-124939 A (Ricoh Co., Ltd.), 25 April, 2003 (25.04.03), Par. Nos. [0027] to [0033]; Fig. 3 (Family: none)	1-11
A	JP 03-123137 A (Fujitsu Ltd.), 24 May, 1991 (24.05.91), Page 5, upper left column, line 1 to lower left column, line 10; Fig. 1 (Family: none)	1-11
A	JP 2001-320373 A (Ricoh Co., Ltd.), 16 November, 2001 (16.11.01), Par. Nos. [0027] to [0031] (Family: none)	1-11

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
18 May, 2004 (18.05.04)

Date of mailing of the international search report
13 July, 2004 (13.07.04)

Name and mailing address of the ISA/
Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００４９１９

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ⁷　　Ｈ０４Ｌ１２／２８

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ⁷　　Ｈ０４Ｌ１２／２８

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　１９２２－１９９６年
日本国公開実用新案公報　　１９７１－２００４年
日本国登録実用新案公報　　１９９４－２００４年
日本国実用新案登録公報　　１９９６－２００４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	ＪＰ　２００３－１２４９３９　Ａ（株式会社リコー） ２００３．０４．２５，【００２７】－【００３３】，図３ （ファミリーなし）	1-11
A	ＪＰ　０３－１２３１３７　Ａ（富士通株式会社） １９９１．０５．２４，第５頁左上欄第１行－左下欄第１０行， 図１（ファミリーなし）	1-11

☒ C欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 １８．０５．２００４	国際調査報告の発送日 13. 7. 2004
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｘ　９２９９ 中木　努 電話番号　０３－３５８１－１１０１　内線　３５９６

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００４９１９

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　２００１－３２０３７３　Ａ（株式会社リコー） ２００１．１１．１６，【００２７】－【００３１】 （ファミリーなし）	1-11